Czytnik kart mikroprocesorowych:

a. Czytnik kart mikroprocesorowych jako urządzenie wewnętrzne (wbudowane) komputera podłączony przez wewnętrzny port USB 2.0.
b. Czytnik kart musi być zgodny ze standardem PC/SC.
c. Czytnik kart musi być zgodny ze standardem Microsoft WHQL (Microsoft Windows Hardware Quality Labs).
d. Czytnik musi umożliwiać odczyt dostępnych na rynku kart kryptograficznych zgodnych z normą ISO-7816, a w szczególności umożliwiać współpracę z kartą w standardzie PKCS#11 co najmniej w wersji 2.01.
e. Czytnik musi posiadać sygnalizację optyczną (np. diodową) akceptacji karty, pracy z kartą.
f. Czytnik musi współpracować z oferowanymi kartami mikroprocesorowymi.

UWAGA: Oferowane czytniki kart mikroprocesorowych i karty mikroprocesorowe mają współpracować z posiadanym przez Policję Centralnym Policyjnym Systemem Autoryzacji funkcjonującym w Policyjnej Sieci Transmisji Danych.
Współpracujące czytniki to:

- **Czytnik Kart Procesorowych Delta-Seck firmy PACOMP sp. z o.o., ul. Puławska 34, Piaseczno**
- **Posnet USB Smartcard Leader firmy POSNET POLSKA S.A., ul. Municypalna 33, Warszawa**
- **Czytnik firmy Digilab sp. z o.o. Aleje Jerozolimskie 200, Warszawa**
- **Czytnik Kart SCR333 firmy SCM Microsystems CryptoTech sp. z o.o. , ul. Wadowicka 6E Kraków**

Współpracująca karta to:

CryptoCard MultiSIGN z chipem SLE 66CX320P sformatowana do podpisu niekwalifikowanego

KARTA MIKROPROCESOROWA:
Wymagania dotyczące kart mikroprocesorowych:

1. Karta musi współpracować z systemami operacyjnymi Microsoft Windows 2000/XP.
2. Karta musi realizować algorytmy RSA i 3DES.
3. Karty muszą być zgodne z normą ISO-7816 część 1,2,3,4,8.
4. Obszar pamięci na klucze prywatne, certyfikaty i inne obiekty nie może być mniejszy niż 32 KB.
5. Karta musi realizować podpis RSA przy użyciu klucza prywatnego znajdującego się na karcie. Zaimplementowany algorytm RSA musi być zgodny ze specyfikacją PKCS#1 w wersji 1.5.
6. Wraz z kartą musi być dostarczona biblioteka dynamiczna DLL dla systemów Windows 2000/XP z implementacją interfejsu PKCS#11 w wersji co najmniej 2.01. Implementacja interfejsu musi być zgodna ze standardem PKCS#11 opublikowanym przez firmę RSA SECURITY.
7. Dostarczona karta mikroprocesorowa musi umożliwiać wygenerowanie nowej pary kluczy RSA, zapis klucza prywatnego, realizację podpisu RSA oraz zapis certyfikatu na kartę.
8. Generator liczb losowych dla generowania kluczy na karcie oparty na zjawisku fizycznym.
9. Karta musi umożliwić przechowywanie co najmniej czterech kluczy prywatnych o długości co najmniej 1024 bity wraz z ich certyfikatami.
10. Karta musi umożliwiać elastyczne definiowanie profilu definiującego zasady kontroli dostępu do obiektów chronionych na karcie, w tym co najmniej:
    a) Możliwość definiowania min. 3 odrębnych kodów PIN oraz związanych z nimi 3 odrębnych kodów PUK (odblokowanie zablokowanego kodu PIN)

b) Możliwość definiowania min. i max długości każdego kodu PIN oraz PUK oraz ilości błędnych prób ich podawania, po których następuje zablokowanie dostępu do kluczy prywatnych i obiektów danych chronionych danym kodem

c) Możliwość definiowania ilości operacji dostępu do danych, na którą ważne jest jednorazowe podanie danego kodu PIN (1, kilka operacji, brak limitu)

d) Możliwość swobodnego wybierania podczas generowania lub zapisywania danych kodu PIN, który będzie chronił dostępu do tych danych

e) Możliwość zapewnienia, iż końcowy użytkownik karty jest jedyną osobą, która posiada dostęp do kluczy prywatnych wygenerowanych na jego karcie

f) Możliwość zabezpieczonej, ponownej inicjalizacji zablokowanej karty bez możliwości dostępu do zablokowanych sekretów (karta z zablokowanymi kodami PUK może być sformatowana i ponownie użyta ale obiekty zablokowane ulegają bezpowrotnemu skasowaniu)

11. Karta musi umożliwiać generowanie wewnątrz oraz zapis z zewnątrz kluczy symetrycznych 3DES
12. Karta musi umożliwiać zapisywanie dowolnych obiektów danych.
13. Wielokrotne usuwanie i zapisywanie ponownie kluczy kryptograficznych i obiektów danych nie może powodować zmniejszania się dostępnej pamięci na te dane (karta musi zarządzać dynamicznie przydziałem i zwalnianiem pamięci)
14. Karta musi pozwalać na efektywne i elastyczne wykorzystanie pamięci na dane i nie może rezerwować na sztywno obszarów pamięci danych bez ich rzeczywistego wykorzystania (np. nie jest dopuszczalne sztywne definiowanie ilości pamięci przeznaczonej na klucze, certyfikaty, dowolne dane)
15. Definiowanie profilu pamięci karty, ilości kodów PIN/PUK, ich parametrów (długości, ilości błędnych prób, itd) musi być możliwe wielokrotnie przez Zamawiającego.
16. Certyfikat bezpieczeństwa układu mikroprocesorowego karty musi posiadać przynajmniej jeden z wymienionych poziomów: ITSEC E3 HIGH lub Common Criteria EAL4 lub FIPS 140-Level3
17. Karta musi być bezterminowa (nie posiada terminu ważności).
18. Karta musi umożliwić uwierzytelnianie w przeglądarce Internet Explorer za pośrednictwem interfejsu MS CSP.
19. Karta udostępniana przez oba interfejsy (PKCS#11 i MS CSP) musi umożliwiać pracę wieloaplikacyjną (jednoczesne używanie karty przez wiele aplikacji). Klucze i obiekty danych zapisywane za pośrednictwem jednego interfejsu muszą być dostępne dla drugiego interfejsu.
20. Dostarczone interfejsy muszą wspierać mechanizm czasowo dostępnego eksportu wygenerowanego klucza prywatnego przez oba interfejsy programowe (do czasu zamknięcia sesji) w celu realizacji funkcji „key backup”
21. Wsparcie dla możliwości jednoczesnego uwierzytelnienia do wszystkich kluczy chronionych oddzielnymi kodami PIN (np. uwierzytelniającego klucza SSL i klucza podpisującego dokument elektroniczny) – utrzymanie uwierzytelnienia do jednego klucza prywatnego podczas uwierzytelniania do innych kluczy
22. Dla obsługi automatycznej personalizacji i inicjalizacji karty przez Policyjne Centrum Autoryzacji wymagane jest dostarczenie biblioteki dynamicznej DLL dla Windows2000/XP/2003 realizującej pełną inicjalizację karty wg wybranego profilu, za pośrednictwem czytnika zgodnego ze standardem PC/SC. Oferenci muszą dostarczyć narzędzia w postaci bibliotek programistycznych, umożliwiających w procesie automatycznej generacji kart możliwość ponownego uaktywnienia zablokowanych kart po wyczerpaniu błędnych kombinacji PIN i PUK przed ponowną personalizacją.
23. W przypadku zaoferowania innej karty niż wskazane w niniejszym załączniku wykonawca zobowiązany jest dostarczyć z ofertą opis dostępnych parametrów zawartych w pliku konfigurującym profil inicjowanej karty.